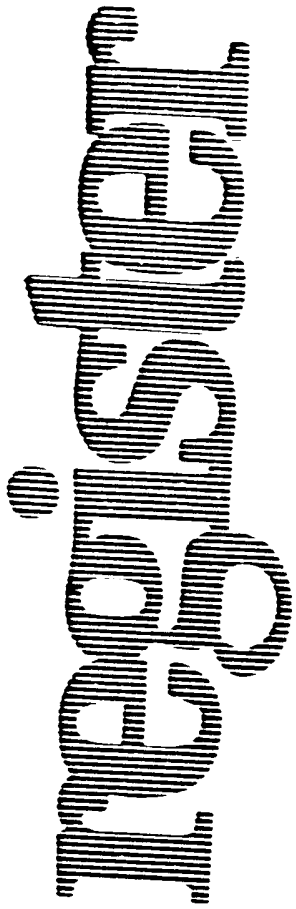

Wednesday
May 16, 1984

Part III

Information Security Oversight Office

32 CFR Part 2001
National Security Information; Final Rule

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2001

National Security Information

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: The Information Security Oversight Office is publishing this amendment to its Directive No. 1, implementing Executive Order 12356 (47 FR 14874, April 6, 1982), pursuant to section 5.2(b)(1) of the Executive Order. The National Security Council approved the issuance of this amendment on May 8, 1984. This amendment to § 2001.47 provides instructions to agencies on the preparation of damage assessments following the loss or possible compromise of national security information.

EXECUTIVE DATE: May 16, 1984.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO (202) 535-7251.

SUPPLEMENTARY INFORMATION: This amendment to ISOO Directive No. 1 is issued pursuant to section 5.2(b)(1) of Executive Order 12356.

List of Subjects in 32 CFR Part 2001

Classified information.

PART 2001—[AMENDED]

32 CFR Part 2001 is amended by revising § 2001.47 to read as follows:

§ 2001.47 Loss or Possible Compromise [4.1(b)].

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The following guidelines shall govern the conduct of damage assessments:

(a) *Initiation of Damage Assessments.* An agency head shall initiate a damage assessment whenever there has been a compromise of classified information originated by that agency that, in his or her judgment, can reasonably be expected to cause damage to the national security. Compromises may occur through espionage, unauthorized disclosures to the press or other members of the public, unauthorized sales, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

(b) *Content of Damage Assessments.* At a minimum, damage assessments shall be in writing and contain the following:

(1) Identification of the source, date, and circumstances of the compromise.

(2) Classification of the specific information lost.

(3) A description of the specific information lost.

(4) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(5) An assessment of the possible advantage to foreign powers resulting from the compromise.

(6) An assessment of whether (i) the classification of the information involved should be continued without change; (ii) the specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; (iii) downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change.

(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(8) An assessment of other appropriate corrective, administrative, disciplinary or legal actions.

(c) *System of Control of Damage Assessments.* Each agency shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in paragraph (a), and that records are maintained in a manner that facilitates their retrieval and use within the agency.

(d) *Cases Involving More Than One Agency.* (1) Whenever a compromise involves the classified information or interests of more than one agency, each department or agency undertaking a damage assessment shall advise other agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment.

(2) Whenever a compromise occurs within an agency that is not responsible for the damage assessment, that agency shall provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

(3) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, the agency performing the damage assessment shall ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

(4) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with appropriate agency legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment shall coordinate with the Department of Justice.

(5) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of Sensitive Compartmented Information (SCI) has occurred.

(Sec. 5.2(b)(1), E.O. 12356)

Dated: May 11, 1984.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 84-13148 Filed 5-15-84; 8:45 am]

BILLING CODE 6820-AF-M